UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/660,368 | 09/11/2003 | Robert Victor Rietveld | 702-030500 | 5466 |

28289 7590 06/21/2006

THE WEBB LAW FIRM, P.C.
700 KOPPERS BUILDING
436 SEVENTH AVENUE
PITTSBURGH, PA 15219

| EXAMINER | |
|---|---|
| PAIK, STEVE S | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2876 | |

DATE MAILED: 06/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/660,368 | RIETVELD, ROBERT VICTOR | |
| | Examiner | Art Unit | |
| | Steven S. Paik | 2876 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *31 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-26 and 30-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *26 and 30-35* is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

### *Continued Examination Under 37 CFR 1.114*

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on March 31, 2006 has been entered.

### *Response to Amendment*

2. Receipt is acknowledged of the Amendment filed October 3, 2005.

### *Claim Rejections - 35 USC § 103*

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-23 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burger (US 6,219,439 B1) in view of Haala (US 6,971,031 B2).

Re claim 1, Burger discloses a system (40) for uniquely identifying an entity (user), comprising:

at least one portable wireless identification device (smart card 14; col. 4, ll. 62-67) having at least one controller mechanism (microprocessor) for wireless communication (col. 5, ll. 1-3) and configured to acquire, process and/or transmit data signals (col. 5, ll. 24-40);

a reader device (12) having:

(i) at least one controller mechanism (col. 5, ll. 13-15) configured to acquire, process and/or transmit data signals; and

(ii) a sensing mechanism (16 and 17) in communication with the reader device controller mechanism and configured to acquire, process and/or transmit data transmitted from the wireless identification device controller mechanism (col. 5, ll. 6-18 and col. 8, ll. 16-28);

at least one wireless control device (48; col. 3, ll. 9-12; and col. 6, ll.1-5 disclose that the connection within the system 40 maybe wired or wireless.) having at least one controller mechanism (CPU) for wireless communication with the reader device controller mechanism and configured to acquire, process and/or transmit data signals, wherein the wireless control device controller mechanism is further configured to:

(i) communicate with and configure the reader device controller mechanism;

(ii) communicate with and configure the wireless identification device controller mechanism via the reader device controller mechanism; and/or

(iii) communicate with and configure subsequent wireless identification device controller mechanism via the reader device controller mechanism (col. 6, line 39 – col. 8, line 43).

However, Burger dose not explicitly disclose the at least one wireless control device is portable. Burger discloses the authentication system including a portable reader (12) that communicates with a PC 48.

Haala discloses a method and system for preventing or obstructing a person from negotiating a transaction with another person, group, or entity in a population, includes verifying and crosschecking the identity of the person and the status of the national identification card carried by the person. The method and system further comprises a remote computer (14) that is

connected with a card reader (12) via a communication link that can be wired, wireless, or through the World Wide Web. It is well known that a computer may include any sizes and shapes from a large size server to a desktop, notebook, handheld, or palm-held size. It is obvious that the smaller size computers such as notebook, handheld, or palm-held size connected in a wireless manner provides portability and mobility to its users to enhance productivity and convenience. Furthermore, Haala discloses that a threshold value for a successful transaction may be modified/or reconfigured based on a level of security as needed.

Therefore, it would have been obvious at the time the invention was made to a person having ordinary skill in the art to substitute the PC (48) of Burger with a remote computer, as taught by Haala, in particular a small size computer specified above to increase productivity and convenience of the identification verification system.

Re claim 2, Burger in view of Haala discloses the system as recited in rejected claim 1 stated above, wherein in operation, the wireless control device controller mechanism wirelessly communicates specified data signals to the reader device controller mechanism and the reader device performs an action sequence based upon the data signals (col. 6, line 39 – col. 8, line 43).

Re claim 3, Burger in view of Haala discloses the system as recited in rejected claim 2 stated above, wherein the data signals are control signals and the action sequence includes communicating with and configuring at least one of the reader device controller mechanism and the wireless identification device controller mechanism (col. 6, line 39 – col. 8, line 43).

Re claim 4, Burger in view of Haala discloses the system as recited in rejected claim 3 stated above, wherein the configuration of the at least one of the wireless identification device

controller mechanism (microprocessor embedded within a smart card 14) and the reader device controller (various chips) includes at least one of:

(i) storing a unique identification (biometric data) value representative of the identity of the wireless identification device on at least one of the reader device controller mechanism and the wireless identification device controller mechanism (col. 5, ll. 6-41); and

(ii) erasing at least a portion of the data on at least one of the reader device controller mechanism and the wireless identification device controller mechanism.

Re claim 5, Burger in view of Haala discloses the system as recited in rejected claim 3 stated above, further comprising a scanner device (a semi-conductor chip 17 constructed to extract biometric data, such as a fingerprint and scan the data as well.) in communication with the reader device controller mechanism (A comparison means (chip) 19 includes a control means (chip) and is connected to the chip 17. The comparison chip compares the data and biometric features of the user. The control chip controls communications at the reader so that the information about the user is not released to an external source before the user authentication is confirmed.) and configured to acquire, process and/or transmit data signals representative of at least one unique characteristic (biometric data of a user) of the entity (user).

Re claim 6, Burger in view of Haala discloses the system as recited in rejected claim 5 stated above, wherein the entity is a person (user) and the unique characteristic is a biometric property of the person (see above).

Re claim 7, Burger in view of Haala discloses the system as recited in rejected claim 6 stated above, wherein the biometric property is one of a fingerprint, a retinal print, and a dermal sample (col. 5, ll. 10-13).

Re claim 8, Burger in view of Haala discloses the system as recited in rejected claim 5 stated above, wherein the configuration of the wireless identification device controller mechanism (microprocessor) includes:

(i) storing the data representative of the unique characteristic of the entity on at least one of the wireless identification device controller mechanism and the reader device controller mechanism (col. 5, ll. 24-40); and/or

(ii) erasing at least a portion of the data representative of the unique characteristic of the entity on at least one of the wireless identification device controller mechanism and the reader device controller mechanism.

Re claim 9, Burger in view of Haala discloses the system as recited in rejected claim 2 stated above, wherein the data signals are control signals and the action sequence includes communicating with a subsequent wireless control device controller mechanism (col. 6, line 39 – col. 8, line 43).

Re claim 10, Burger in view of Haala discloses the system as recited in rejected claim 9 stated above, wherein the action sequence includes at least one of reading, configuring and verifying the subsequent wireless control device (col. 6, line 39 – col. 8, line 43).

Re claim 11, Burger in view of Haala discloses the system as recited in rejected claim 1 stated above, further comprising a structure integrated controller mechanism in communication with the reader device controller mechanism and configured to acquire, process and/or transmit data signals (Fig. 2).

Re claim 12, Burger in view of Haala discloses the system as recited in rejected claim 11 stated above, wherein, in operation, at least one of the wireless identification device controller

mechanism and the wireless control device controller mechanism wirelessly communicates specified data signals to the reader device controller mechanism and the reader device performs an action sequence based upon the data signals (col. 6, line 39 – col. 8, line 43).

Re claim 13, Burger in view of Haala discloses the system as recited in rejected claim 12 stated above, wherein the structure integrated controller mechanism is in communication with a lock mechanism (42) which, in turn, is in communication with an access point (access door 44) and is configured to prevent access through the access point and the action sequence is temporarily disabling (col. 6, ll. 1-5 and ll. 39-67) the lock mechanism.

Re claim 14, Burger in view of Haala discloses the system as recited in rejected claim 11 stated above, further comprising a scanner device (a semi-conductor chip 17 constructed to extract biometric data, such as a fingerprint and scan the data as well.) in communication with the reader device controller mechanism (A comparison means (chip) 19 includes a control means (chip) and is connected to the chip 17. The comparison chip compares the data and biometric features of the user. The control chip controls communications at the reader so that the information about the user is not released to an external source before the user authentication is confirmed.) and configured to acquire, process and/or transmit data signals representative of at least one unique characteristic (biometric data of a user) of the entity (user).

Re claim 15, Burger in view of Haala discloses the system as recited in rejected claim 14 stated above, wherein the entity is a person (user) and the unique characteristic is a biometric property of the person (see above).

Re claim 16, Burger in view of Haala discloses the system as recited in rejected claim 15 stated above, wherein the biometric property is one of a fingerprint, a retinal print, and a dermal sample (col. 5, ll. 10-13).

Re claim 17, Burger in view of Haala discloses the system as recited in rejected claim 11 stated above, wherein, in operation, at least one of the wireless identification device controller mechanism and the wireless control device controller mechanism wirelessly communicates specified data signals to the reader device controller mechanism and the reader device performs an action sequence based upon the data signals, including data representative of at least one unique characteristic of the entity (col. 6, line 39 – col. 8, line 43).

Re claim 18, Burger in view of Haala discloses the system as recited in rejected claim 17 stated above, wherein the structure integrated controller mechanism is in communication with a lock mechanism (42) which, in turn, is in communication with an access point (access door 44) and is configured to prevent access through the access point and the action sequence is temporarily disabling (col. 6, ll. 1-5 and ll. 39-67) the lock mechanism.

Re claim 19, Burger in view of Haala discloses the system as recited in rejected claim 1 stated above, wherein at least one of the wireless identification device and the wireless control device is in the form of a portable card (smart card 14).

Re claim 20, Burger in view of Haala discloses the system as recited in rejected claim 1 stated above, wherein at least one of the wireless identification controller mechanism, the reader device controller mechanism and the wireless control device controller mechanism are in the form of a printed circuit board (The chip is an integrated circuit chip and PC 48 comprises a plurality of PCB's).

Re claim 21, Burger in view of Haala discloses the system as recited in rejected claim 1 stated above, wherein the reader device (12) is in the form of an enclosed housing having at least a portion (input 18 in a wired communication; a transceiver may be used in a wireless communication) configured to allow for the acquisition and transmission of data signals therethrough.

Re claim 22, Burger in view of Haala discloses the system as recited in rejected claim 21 stated above, wherein the reader device (12) further includes at least one of an audio indication device (col. 5, ll. 63-65) and a visual indication device (34 and 36) in communication with and controlled by the reader device controller mechanism.

Re claim 23, Burger in view of Haala discloses the system as recited in rejected claim 22 stated above, wherein the audio indication device (col. 5, ll. 63-65) is in the form of a speaker and the visual indication device is in the form of a plurality of LEDS (Burger discloses that if authentication is confirmed to be positive, a visual indicator 34 will light. If it is determined that the data at the fingerprint scanner 16 does not correspond to that which is stored in the chip memory 22, an indicator 36 will be lit. Other visual indicators may also be used to indicate transmissions and receptions of data, after authentication of the user is positively confirmed.

Although neither Burger nor Haala specifically discloses a type of light source used in the reader to indicate a status of authentication, the references do not limit to a particular type of a visual indicator. LED's are commonly used in the filed of computing devices to indicate a status of the devices. Usually a green LED is for successful or acceptable result and a red LED for unsuccessful or unacceptable result. Burger uses two visual indicators 34 and 36 to distinctively indicate different authentication status.

Therefore, it would have been obvious at the time the invention was made to a person having ordinary skill in the art to incorporate a plurality of LED's, preferably with different colors, to indicate a status of authentication. The LED's with different color would undoubtedly provide a quick visual confirmation of an authentication process. Furthermore, LED's are inexpensive compared to other types of visual indicators such as an LCD.

With respect to claim 25, Burger discloses a system (40) for uniquely identifying an entity (user), comprising:

at least one portable wireless identification device (smart card 14) having at least one controller mechanism (microprocessor) for wireless communication and configured to acquire, process and/or transmit data signals (control signals and biometric data);

a reader device (12) having:

(i) at least one controller mechanism (col. 5, ll. 13-15) configured to acquire, process and/or transmit data signals; and

(ii) a sensing (16 and 17) mechanism in communication with the reader device controller mechanism and configured to acquire, process and/or transmit data transmitted from the wireless identification device controller mechanism (col. 5, ll. 6-18 and col. 8, ll. 16-28);

at least one wireless control device (48; col. 3, ll. 9-12; and col. 6, ll.1-5 disclose that the connection within the system 40 maybe wired or wireless.) having at least one controller mechanism (CPU) for wireless communication with the reader device controller mechanism and configured to acquire, process and/or transmit data signals, wherein the wireless control device controller mechanism is further configured to:

(i) communicate with and configure the reader device controller mechanism;

(ii) communicate with and configure the wireless identification device controller mechanism via the reader device controller mechanism; and/or

(iii) communicate with and configure subsequent wireless identification device controller mechanism via the reader device controller mechanism (col. 6, line 39 – col. 8, line 43) ; and

scanner device (a semi-conductor chip 17 constructed to extract biometric data, such as a fingerprint and scan the data as well.) in communication with the reader device controller mechanism (A comparison means (chip) 19 includes a control means (chip) and is connected to the chip 17. The comparison chip compares the data and biometric features of the user. The control chip controls communications at the reader so that the information about the user is not released to an external source before the user authentication is confirmed.) and configured to acquire, process and/or transmit data signals representative of at least one unique characteristic of the entity;

wherein the data signals include control signals and an action sequence includes communicating with and configuring at least one of the reader device controller mechanism and the wireless identification device controller mechanism,

wherein the configuration of the wireless identification device controller mechanism includes:

(i) storing the data representative of the unique characteristic of the entity on at least one of the wireless identification device controller mechanism and the reader device controller mechanism (col. 5, ll. 6-41); and/or

(ii) erasing at least a portion of the data representative of the unique characteristic of the entity on at least one of the wireless identification device controller mechanism and the reader device controller mechanism.

However, Burger dose not explicitly disclose the at least one wireless control device is portable.

Haala discloses a method and system for preventing or obstructing a person from negotiating a transaction with another person, group, or entity in a population, includes verifying and crosschecking the identity of the person and the status of the national identification card carried by the person. The method and system further comprises a remote computer (14) that is connected with a card reader (12) via a communication link that can be wired, wireless, or through the World Wide Web. It is well known that a computer may include any sizes and shapes from a large size server to a desktop, notebook, handheld, or palm-held size. It is obvious that the smaller size computers such as notebook, handheld, or palm-held size connected in a wireless manner provides portability and mobility to its users to enhance productivity and convenience. Furthermore, Haala discloses that a threshold value for a successful transaction may be modified/or reconfigured based on a level of security as needed.

Therefore, it would have been obvious at the time the invention was made to a person having ordinary skill in the art to substitute the PC (48) of Burger with a remote computer, as taught by Haala, in particular a small size computer specified above to increase productivity and convenience of the identification verification system.

5. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Burger (US 6,219,439 B1) as modified by Haala (US 6,971,031 B2) as applied to claim 1 above, and further in view of Lane (US 5,623,552)..

The teachings of Burger in view of Haala have been fully discussed above with the exception of specifically disclosing the wireless identification device and the wireless control device, and the respective controller mechanisms, is integrated in a single portable medium.

Lane discloses a self-authenticating identification card comprising a fingerprint sensor for authenticating the identity of a user. The portable integrated identification card allows its carrier positive identity verification without requiring an external equipment while improving the security of the identification card.

Therefore, it would have been obvious at the time the invention was made to a person having of ordinary skill in the art to employ a portable integrated identification card as taught by Lane into the teachings of Burger in view of Haala for the purpose of simplifying authentication process and preventing a fraudulent activity if the card is lost or stolen.

***Allowable Subject Matter***

6. Claims 26 and 30-35 are allowable.

7. The following is a statement of reasons for the indication of allowable subject matter: none of the cited prior art of the record discloses, teaches, or fairly suggests the claimed limitation recited in claim 26 including a step of controlling, by the wireless control device, the storage of the data representative of the unique characteristic of the entity on the wireless identification device, via the reader device, and the erasure of the data representative of the unique characteristic of the entity from the reader device and/or the wireless control device.

***Response to Arguments***

8. Applicant's arguments filed March 312, 2006 have been fully considered but they are not persuasive.

The applicant amended claims by deleting "at least one of" in one of recited elements or steps and added "and/or" in claims 1, 8, and 25. It is appeared that the amended claims are essentially the same as the original claims. Therefore, the examiner maintained the rejection as discussed above.

The applicant argues that none of the cited prior art teaches or suggests a portable wireless control device with the claimed control features. The examiner respectfully disagrees. Burger discloses a PC (48) that functions as a wireless control device (based on a type of network such as wired or wireless). Haala reference discloses a type of PC that can be used in place of PC (48) of Burger. Therefore, the argument is not persuasive.

The examiner believes claims 26 and 30-35 are allowable over cited prior art.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Steven S. Paik whose telephone number is 571-272-2404. The examiner can normally be reached on Monday - Friday 5:30a-2:00p (Maxi-Flex*).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on 571-272-2398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Steven S. Paik
Primary Examiner
Art Unit 2876

ssp